<u>IN THE CLAIMS</u>

Please amend the claims as follows:

Claims 1-3 (Canceled).

Claim 4 (Currently Amended): A method of <u>detecting</u> ~~generating a computer readable user identification number of a colluder who made a collusion attack on a computer readable content~~ <u>watermark information embedded in a content, the watermark information being a concatenation of component codes</u> ~~by detecting a computer readable embedded code which is embedded in the computer readable content and is a concatenation of a plurality of computer readable component codes~~, <u>the method</u> comprising:

receiving said ~~predetermined~~ content ~~which contains the computer readable embedded code therein~~ from an external device;

detecting said <u>watermark information from the received content</u> ~~computer readable embedded code contained within said computer readable content~~;

dividing the <u>detected watermark information</u> ~~computer readable embedded code~~ into the ~~plurality of computer readable~~ component codes;

decoding each of the ~~plurality of computer readable~~ component codes, thereby to obtain a plurality of residues pairs each comprising two residues, taking a plurality of <u>predetermined</u> integers which ~~are predetermined and~~ are relatively prime to each other, as moduli;

calculating ~~the computer readable~~ user identification ~~number~~ of [[the]] <u>a</u> colluder <u>who made a collusion attack on the content</u>, from the plurality of residue pairs; and

outputting said calculated ~~computer readable~~ user identification ~~number~~, wherein

the ~~plurality of component computer readable~~ codes are component codes that have a

possibility to have a method of decoding at least one of the residues with respect to the

~~computer readable~~ user identification ~~number~~ of the colluder.

Claim 5 (Currently Amended): An apparatus for <u>detecting</u> ~~generating a computer~~

~~readable user identification number of a colluder who made a collusion attack on a computer~~

~~readable content~~ <u>watermark information embedded in a content, the watermark information</u>

<u>being a concatenation of component codes</u> ~~by detecting a computer readable embedded code~~

~~which is embedded in the computer readable content and is a concatenation of a plurality of~~

~~computer readable component codes,~~ <u>the apparatus</u> comprising:

an input port configured to receive said ~~predetermined~~ content ~~which contains the~~

~~computer readable embedded code therein~~ from an external device;

a detector configured to detect said <u>watermark information from the received content</u>

~~computer readable embedded code contained within said computer readable content~~;

a code divider configured to divide the <u>watermark information</u> ~~computer readable~~

~~embedded code~~ into the ~~plurality of computer readable~~ component codes;

a component code decoder configured to decode each of the ~~plurality of computer~~

~~readable~~ component codes, thereby to obtain a plurality of residues pairs each comprising two

residues, taking a plurality of <u>predetermined</u> integers which are ~~predetermined and are~~

relatively prime to each other, as moduli;

a colluder number calculator configured to calculate ~~the computer readable~~ user

identification ~~number~~ of [[the]] <u>a</u> colluder <u>who made a collusion attack on the content</u>, from

the plurality of residue pairs; and

an output port configured to output said calculated ~~computer readable~~ user

identification ~~number~~, wherein

the ~~plurality of computer readable~~ component codes are component codes that have a

possibility to have a method of decoding at least one of the residues with respect to the

~~computer readable~~ user identification ~~number~~ of the colluder.

Claim 6 (Currently Amended): An apparatus according to claim 5, wherein the

plurality of ~~computer readable~~ component codes are each constructed by continuous

sequences of 1 and 0, taking a predetermined number of bits as a unit.

Claim 7 (Currently Amended): An apparatus according to claim 5, further

comprising:

a collusion determiner configured to determine presence or absence of a collusion

from the plurality of residue pairs, wherein

the colluder identification number calculator is configured to calculate the ~~computer~~

~~readable~~ user identification number of the colluder, if presence of a collusion is determined

by the colluder determiner.

Claim 8 (Currently Amended): An apparatus according to claim 5, wherein the

colluder number calculator includes:

a residue selecting section configured to select one residue from each of k' inputted

residues pairs, thereby to generate a set of k' residues (R1, R2, ..., Rk');

a Chinese remainder theorem section configured to calculate a candidate of a

~~computer readable~~ user identification number u of a colluder, from k residues (S1, S2, ..., Sk)

which are different from each other and selected from the set of k' residues generated by the

residue selecting section, in accordance with a Chinese remainder theorem; and

a consistency checking section [[is]] configured to select the k residues from the set of

k' residues generated by the residue selecting section, configured to supply the k residues to

the Chinese remainder theorem section, configured to specify a user identification number of

the colluder from the candidate of the user identification number u of the colluder calculated

by the Chinese remainder theorem section, and configured to output the user identification

number of the colluder, wherein

the consistency checking section has selection processing configured to select the k

residues from the set of k' residues generated by the residue selecting section, determination

processing configured to determine whether or not a relationship of Ri=u mod pi (i=i_1, i_2, ...,

i_ℓ) exists between the candidate of the computer readable user identification number u of the

colluder calculated by the Chinese remainder theorem section and a predetermined number

(ℓ) of residues among remaining (k'-k) residues, and output processing configured to output

the candidate as a ~~computer readable~~ user identification number of a colluder if the

relationship exists as a result of the determination processing, <u>wherein</u>

if the relationship does not exist, a new combination of k residues (S 1, S2, ..., Sk) is

selected from the set of the k' residues generated by the residue selecting section, thereby to

carry out the determination processing, and if the relationship does not exist with respect to

any of all combinations of k residues (S1, S2, ..., Sk), a new set of k' residues is requested to

the residue selecting section, and the selection processing and the determination processing

are repeated until the relationship exists.

Claims 9-13 (Canceled).

Claim 14 (Currently Amended): An apparatus <u>detecting</u> ~~generating a computer~~

~~readable user identification number of a colluder who made a collusion attack on a computer~~

~~readable content~~ watermark information embedded in a content, the watermark information being a concatenation of component codes respectively generated in correspondence with user identifications, the component codes being such that among k' component codes capable of expressing all sets of integral elements calculated with respect to a predetermined number of user identifications and k combinations of the k' component codes can uniquely express the user identifications ~~by detecting a computer readable embedded code~~, the apparatus comprising:

an input port configured to receive from an external device said ~~predetermined~~ content ~~having the computer readable embedded code embedded therein~~;

a detector configured to detect said watermark information from the received ~~computer readable embedded code contained within said computer readable~~ content;

~~a code extractor configured to extract the computer readable embedded code from the computer readable content, the computer readable embedded code is a concatenation of a plurality of computer readable component codes respectively generated in correspondence with an inputted computer readable user identification number and also being such that among k' computer readable component codes capable of expressing all sets of integral elements that are calculated with respect to a predetermined number of computer readable user identification numbers, k combinations of the k' computer readable component codes can uniquely express the user identification numbers;~~

a code divider configured to divide the watermark information into the ~~perform a division and extract computer readable~~ component codes;

a component code decoder configured to decode each of the ~~extracted computer readable~~ component codes;

a colluder number calculator configured to calculate ~~a computer readable~~ user identification ~~number~~ of a colluder <u>who made a collusion attack on the content</u> from a decoding result of each of the ~~computer readable~~ component codes; and

an output port configured to output said ~~computer readable~~ user identification ~~number~~, wherein

k' is determined to be c(k+ℓ)/q or more where c is a positive integer of 3 or more, ℓ is a positive integer, and q is a number of the integral elements which can be detected from each of the ~~computer readable~~ component codes when detecting the ~~computer readable~~ embedded code.

Claim 15 (Currently Amended): An apparatus according to claim 14, wherein, where pi (i=1, 2, ..., k') is a number of values which each of the integral <u>elements</u> ~~factors~~ calculated by the <u>colluder number</u> calculator can take with respect to the predetermined number of ~~computer readable~~ user identification numbers and where ε is a detection error rate which is assumed when detecting the ~~computer readable~~ embedded code, k' is determined such that a condition of

$$\left[1 - \prod_{i=l}^{l}\left\{1 - \left(1 - \frac{1}{pi}\right)^{c}\right\}\right]^{c(k+l)/2^{c_{k+l}} X 2^{k+l}} \geq 1 - \frac{\varepsilon}{2}$$

is satisfied.

Claim 16 (Currently Amended): An apparatus according to claim 14, wherein the set of integral elements is a set of residues, which are calculated in correspondence with the ~~computer readable~~ user identification number and take a plurality of integers relatively prime to each other as moduli.

Claim 17 (Currently Amended): An apparatus according to claim 14, wherein the set of integral elements is a set of numbers of elements which are calculated in correspondence with the ~~computer-readable~~ user identification number and belong to an equivalence class defined by a parallel transformation.

Claim 18 (Currently Amended): An apparatus according to claim 14, wherein the set of integral elements is a set of numbers of elements which are calculated in correspondence with the ~~computer-readable~~ user identification number and belong to an equivalence class defined by a parallel transformation, and

where p_i (i=1, 2, ..., k') is one same positive integer p, a condition of

$$k' = \frac{c}{2}(k + l) \le \frac{p^k - 1}{p - 1}$$

is further satisfied.

Claim 19 (Currently Amended): An apparatus for <u>detecting</u> ~~generating a computer readable user identification number of a colluder who made a collusion attack on a computer readable content~~ <u>watermark information embedded in a content, the watermark information being a concatenation of component codes respectively generated in correspondence with user identifications, the component codes being such that among k' component codes capable of expressing all sets of integral elements calculated with respect to a predetermined number of user identifications and k combinations of the k' component codes can uniquely express the user identifications</u> ~~by detecting a computer readable embedded code~~, <u>the apparatus</u> comprising:

8

an input port configured to receive from an external device ~~computer readable~~ the

content ~~having the computer readable embedded code embedded therein~~;

a detector configured to detect said <u>watermark information from the received</u>

~~computer readable embedded code from said computer readable~~ content;

~~a code extractor configured to extract the computer readable embedded code from~~

~~said computer readable content, the computer readable embedded code is a concatenation of~~

~~computer readable component codes respectively generated in correspondence with an~~

~~inputted computer readable user identification number and also being such that among k'~~

~~computer readable component codes capable of expressing all sets of integral elements that~~

~~are calculated with respect to a predetermined number of computer readable user~~

~~identification numbers, k combinations of the k' computer readable component codes can~~

~~uniquely express the computer readable user identification numbers~~;

a code divider configured to <u>divide the watermark information into the</u> ~~perform a~~

~~division into extracted computer readable~~ component codes;

a component code decoder configured to decode each of the ~~extracted computer~~

~~readable~~ component codes;

a colluder number calculator configured to calculate ~~a computer readable~~ user

identification ~~number~~ of a colluder <u>who made a collusion attack on the content</u> from a

decoding result of each of the ~~computer readable~~ component codes; and

an output port for outputting said ~~computer readable~~ user identification number,

wherein

the component code decoder includes a block dividing section configured to divide

each of the component codes into blocks, a counting section configured to count a number of

bits of "1" in every one of the blocks, a first determining section configured to determine

whether or not a count value obtained by the counting section exceeds a first threshold value,

a second determining section configured to determine whether or not the count value is

smaller than a second threshold value, a minimum position selecting section configured to

select a minimum block determined as exceeding the first threshold value by the first

determining section, and a maximum position selecting section configured to select a

maximum block determined as being smaller than the second threshold value, thereby to

output a selection results of the minimum and maximum position selecting sections, as a

decoding result.

Claims 20-22 (Canceled).

Claim 23 (Currently Amended): An apparatus according to claim 5, wherein the

colluder number calculator is configured to generate at least one ~~computer readable~~ user

identification number candidate having a possibility to be the ~~computer readable~~ user

identification number of the colluder, from the plurality of residue pairs, selects at least one

~~computer readable~~ user identification number having a lower possibility to be erroneously

detected as the ~~computer readable~~ user identification number of the colluder, among the

~~candidate~~ candidates, and decides the selected ~~computer readable~~ user identification number

as the ~~computer readable~~ user identification number of the colluder.

Claim 24 (Currently Amended): An apparatus according to claim 5, wherein the

colluder number calculator is configured to sequentially generate a plurality of ~~computer~~

~~readable~~ user identification number candidates having a possibility to be the computer

readable user identification number of the colluder, from the plurality of residue pairs,

~~determines~~ is configured to determine whether a possibility to be erroneously detected as the

~~computer readable~~ user identification number of the colluder is high or low, with respect to

the candidates, and ~~decides~~ is configured to decide all of the ~~computer-readable~~ user

identification numbers that have the possibility to be determined to be low, as ~~computer~~

~~readable~~ user identification numbers of colluders.

Claim 25 (Currently Amended): An apparatus according to claim 23, wherein the

colluder number calculator is configured to obtain a number of those residues among all of

the residues pairs that satisfy a congruence to the residues taking the plurality of integers as

modulus, with respect to all ~~computer-readable~~ user identification numbers, and is configured

to generate a ~~computer-readable~~ user identification number which makes the number to be a

predetermined threshold value or more, as a ~~computer-readable~~ user identification number

candidate of the colluder.

Claim 26 (Currently Amended): An apparatus according to claim 24, wherein the

colluder number calculator is configured to obtain a number of those residues among all of

the residues pairs that satisfy a congruence to the residues taking the plurality of integers as

modulus, with respect to all ~~computer-readable~~ user identification numbers, and is configured

to generate a ~~computer-readable~~ user identification number which makes the number to be a

predetermined threshold value or more, as a ~~computer-readable~~ user identification number

candidate of the colluder.

Claim 27 (Currently Amended): An apparatus according to claim 5, wherein the

colluder number calculator includes a storage device configured to store a plurality of

~~computer-readable~~ user identification numbers having a lower possibility at which the

plurality of ~~computer-readable~~ user identification numbers are erroneously detected as the

~~computer-readable~~ user identification numbers of the colluder, and is configured to decide a

~~computer readable~~ user identification number which coincides with at least one ~~computer~~

~~readable~~ user identification number candidate having a possibility to be the ~~computer~~

~~readable~~ user identification number of the colluder, generated from the plurality of residue

pairs, among the ~~computer readable~~ user identification numbers stored in the storage device.